

SEALED**UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA****ORIGINAL**

UNITED STATES OF AMERICA

v.

Brandon Quinn Harris,
Aka "John Patriot"

CRIMINAL COMPLAINT

CASE NUMBER: 17-9495 MJ

I, the undersigned complainant, being duly sworn, state that the following is true and correct to the best of my knowledge and belief:

On or about July 26, 2017, in the County of Maricopa in the District of Arizona and elsewhere, BRANDON QUINN HARRIS knowingly transmitted in interstate and foreign commerce from Arizona to Ohio and/or Texas, with intent to extort from the Victim Company money and other things of value, a communication containing a threat to injure the property and reputation of the Victim Company, all in violation of 18 U.S.C. § 875(d).

I further state that I am a Special Agent from the Federal Bureau of Investigation and that this complaint is based on the following facts:

See Attached Statement of Probable Cause Incorporated By Reference Herein.

Continued on the attached sheet and made a part hereof: ☐ Yes ☐ No

AUTHORIZED BY: James R. Knapp, AUSA *JK*

SA, Steven Garbett
Name of Complainant

AD
Signature of Complainant

Sworn to before me and subscribed in my presence

10/31/2017
Date

at

Phoenix, Arizona
City and State

HONORABLE EILEEN S. WILLET
United States Magistrate Judge
Name & Title of Judicial Officer

E. Willett
Signature of Judicial Officer

STATEMENT OF PROBABLE CAUSE

I, Steven Garbett, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed for nine years. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer crimes, including criminal computer intrusions. I have gained experience through training at the FBI Academy, including training pertaining to cyber investigations. I have a bachelor's degree in Computer Information Systems and over 10 years of experience working in Information Technology. I have received training in the area of computer intrusions and have had the opportunity to observe and review numerous cases and methods used by cyber criminals.

2. The facts in this Statement of Probable Cause come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. On February 21, 2017, Robert Jeremy MILLER (hereafter, "MILLER") was terminated from his position at a large technology company headquartered in New Jersey, but with offices across the United States, including in Arizona (hereafter, the "Victim Company"). MILLER's job title at the time of his termination was Senior Project Management Specialist.

4. As a Senior Project Management Specialist, MILLER's duties primarily consisted of administering the Victim Company's proprietary satellite tracking system

(hereafter, the “STS”). The STS was designed to track the location and movements of aircraft and marine craft. Clients of the Victim Company, including commercial organizations, would pay the Victim Company for access to an online system that would allow clients to log in and monitor the location and movements of the clients’ aircraft and/or marine craft. The Victim Company considered MILLER to be the Victim Company’s leading subject-matter expert on the STS. As an administrator of the STS, MILLER had the ability to access the STS remotely and create login IDs for the system; however, after February 21, 2017, the Victim Company removed MILLER’s access to the company computer network when his employment was terminated and deleted all known login IDs that MILLER had for the STS at that time.

5. On July 23, 2017, the Victim Company received a phone call from an individual calling himself “John Patriot.” PATRIOT communicated with the Victim Company using telephone number (317) 220-3777. PATRIOT stated that he had become aware of a man who planned to sell login IDs to access the Victim Company’s “satellites” on the black market. PATRIOT explained that the man to whom he referred claimed to have a level one security and the ability to use temporary login IDs or create permanent IDs to access the Victim Company’s satellite system. Additionally, PATRIOT claimed that the man was looking to sell the login IDs to allow a buyer access to the information and was hoping to obtain five million dollars. According to PATRIOT, the man told PATRIOT that he had worked at the Victim Company and was “pissed that he didn’t get a raise and wanted to screw over the company.”

6. Investigators from the Victim Company followed up with a telephone call to PATRIOT later that day. PATRIOT initially did not give the real name of the individual who sought to sell the STS login IDs. However, after the investigator continued to ask for the individual's real name, PATRIOT stated that the individual's name was "Robert Miller." The investigator asked if the individual's middle initial was "J," and PATRIOT confirmed. PATRIOT stated that PATRIOT "was not looking to get rich," but wanted some compensation for bringing the matter to the Victim Company's attention.

7. PATRIOT provided the Victim Company with screen shots via text message of what PATRIOT claimed to be the STS to show that MILLER had unauthorized access to the computer network. Engineers from the Victim Company confirmed that the screen shots were from the Victim Company's STS and depicted a visual of location data as to one of the Victim Company's client's aircraft and/or marine craft on July 26, 2017. Specifically, one of the screen shots displayed tracking information for one of the Victim Company's client's aircraft on July 26, 2017. PATRIOT advised that he could facilitate a demonstration with MILLER of real-time access to the STS.

8. On July 26, 2017, the Victim Company received multiple telephone calls and text messages from PATRIOT. During the phone and text message conversations, PATRIOT advised that he would report to the media and to the Victim Company's customers that the Victim Company had a leak to the STS system if he was not compensated. When the Victim Company asked what PATRIOT was talking about in

regards to payment, PATRIOT responded that he believed the information would be worth “at least 5 figures.”

9. On July 26, 2017, the Victim Company received a text message from PATRIOT that stated, “You got 1.5 hrs. to get me an offer or I head to the embassy.” The Victim Company received a separate text from PATRIOT that read, “I’m also going to stop at the first news outlet and give them a nice story for the 6pm news.” PATRIOT also sent a text message that stated, “[E]ither you deal with embarrassment in a PR mess and lose the trust from your clients or you pay for my silence.”

10. On July 31, 2017, the Victim Company asked PATRIOT to meet in person to provide proof of his communications with MILLER. PATRIOT agreed and reiterated his expectation of monetary compensation. PATRIOT stated that it would need to be more than \$10,000. PATRIOT warned the Victim Company that he had provided all of the information to his brother and had given him instructions that if PATRIOT did not return from the meeting to release all the information to the media.

11. A public database search for PATRIOT’s phone number, (317) 220-3777, identified an associated Facebook profile for “Quinn Harris,” date of birth August 6, 1975, and listed locations of Arizona and Indianapolis, Indiana. A criminal check for “Quinn Harris” and date of birth August 6, 1975 returned “Brandon Quinn Harris,” date of birth August 6, 1975, and address on W Indian School Road in Phoenix, Arizona.

12. On July 31, 2017, FBI agents, posing as employees of the Victim Company, met with PATRIOT at a public location. Using the motor vehicle division photo for Brandon Harris, the agents positively identified PATRIOT as Brandon Quinn

Harris (hereafter, "HARRIS"). During the meeting, HARRIS said that he had spoken with MILLER about the STS, that MILLER believed he could make money by selling access to the STS on the black market, and that HARRIS had told MILLER he could assist him in locating a potential buyer for the STS. HARRIS advised the FBI that he and MILLER had discussed trying to sell access to the STS to the Mexican cartel. HARRIS stated he had told Miller that he was in contact with the Mexican Cartel and that they were willing to pay two million dollars for access to the STS. However, HARRIS stated that he had, in fact, not been in contact with the Mexican Cartel but had only told Miller that story to hold him off until HARRIS could report this to the Victim Company. HARRIS stated that he was a patriot and was concerned that American lives could be lost if MILLER were to sell the STS access to the real cartel as MILLER had initially proposed.

13. During the meeting, HARRIS again expressed his desire to be paid for the information he was reporting on MILLER. When asked what would happen if he did not get paid for the information, HARRIS stated that it would be "a roll of the dice" and that he could leak the information to the media.

14. At this point in the meeting, the interviewers identified themselves as FBI agents. HARRIS confirmed that his real name was Brandon Quinn Harris and told the agents that he had been communicating with MILLER via HARRIS's cellular telephone, (317) 220-3777. During the meeting, HARRIS had in his possession the telephone utilizing phone number (317) 220-3777. HARRIS opened the telephone and showed the agents text messages he had exchanged with MILLER. HARRIS consented to a search

of his cellular telephone and allowed the agents to take the phone to have it forensically examined. The examination identified multiple text messages between HARRIS and MILLER as well as messages HARRIS had sent to the Victim Company. One of the text messages from MILLER to HARRIS, dated July 23, 2017, included the internet address of the Victim Company's STS access page, and another text message, dated July 23, 2017, included a temporary login ID and password for the STS. After discussing the STS with the Victim Company, your Affiant knows that a temporary login ID for the STS can only be created by accessing Victim Company's system.

15. Additionally, there were text messages between MILLER and HARRIS between July 23, 2017, and July 26, 2017, in which HARRIS and MILLER discussed how much a potential buyer would pay for access to the STS. During the text-message conversation, MILLER asked HARRIS, "What price you think?" And, after HARRIS advised MILLER that he had "an offer for \$500k," MILLER wrote to HARRIS, "Think we should take an offer below 5mill and make em pay a hefty monthly?"

16. An additional text message sent from MILLER to HARRIS, dated July 26, 2017, included a screen shot of the STS. The screen shot was the same as the one previously provided to the Victim Company by HARRIS that displayed tracking information for an aircraft on July 26, 2017.

17. The review of HARRIS' cellular telephone also identified a document on the phone that appeared to be a pay stub from BMH Unlimited for Brandon Q. Harris. The following day, the agents returned the phone to HARRIS at the address listed on his

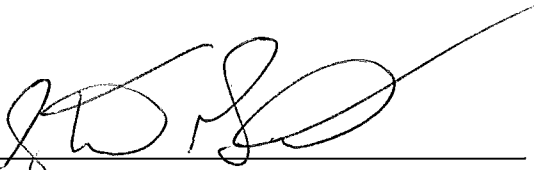
criminal report on W Indian School Road in Phoenix, Arizona. HARRIS answered the door and took custody of the phone. HARRIS stated that he was living there temporarily and would be moving out soon.

18. MILLER was subsequently arrested while trying to sell access to the STS to undercover FBI agents posing as members of the Mexican Cartel. MILLER has been charged in CR-17-1112-PHX-DGC with Unauthorized Access of a Protected Computer to Obtain information, in violation of title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B) and Unauthorized Access of a Protected Computer in Furtherance of Fraud, in violation of title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A).

19. A grand jury subpoena for records related to phone number (317) 220-3777 identified the number as a Verizon Wireless phone number. Verizon confirmed that their company does not have any text message - Short Message Service (SMS) or Multimedia Message Service (MMS) - servers located in Arizona. Verizon MMS message servers are located in Southlake, Texas; Cincinnati, Ohio; and Westland, Texas. MMS messages on the Verizon network are stored on servers in one of these three locations until the message is retrieved by the message recipient.

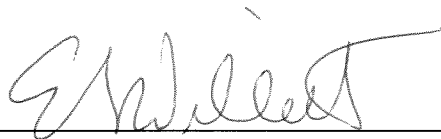
20. Based upon the aforementioned facts, your Affiant believes that probable cause exists that on or about July 26, 2017, in the District of Arizona and elsewhere, HARRIS knowingly transmitted in interstate and foreign commerce from Arizona to Ohio and/or Texas, with intent to extort from the Victim Company money and other things of value, a communication containing a threat to injure the property and reputation of the Victim Company, all in violation of 18 U.S.C. § 875(d).

21. Because Harris's current whereabouts are unknown, I am also requesting that the Court issue an arrest warrant.



STEVEN GARBETT
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 31 day of October, 2017.



HON. EILEEN S. WILLETT
United States Magistrate Judge